

Rebecca Davis (SBN 271662)  
rebecca@lozeaudrury.com  
**LOZEAU DRURY LLP**  
1939 Harrison Street, Suite 150  
Oakland, CA 94612  
Telephone: (510) 836-4200  
Facsimile: (510) 836-4205

Patrick H. Peluso\*  
ppeluso@woodrowpeluso.com  
**WOODROW & PELUSO, LLC**  
3900 East Mexico Avenue, Suite 300  
Denver, CO 80210  
Telephone: (720) 213-0676  
Facsimile: (303) 927-0809

*\*Pro Hac Vice admission to be sought*

*Attorneys for Plaintiff and the alleged Class*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF CALIFORNIA**

**ADRIAN SCOTT RANGLES,**  
individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

**MR. COOPER GROUP, INC.,** a  
Delaware corporation, and  
**NATIONSTAR MORTGAGE, LLC,**  
**d/b/a MR. COOPER,** a Delaware  
limited liability company, and

Defendants.

Case No:

**CLASS ACTION COMPLAINT  
JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Adrian Scott Randles (“Plaintiff” or “Randles”) brings this Class Action Complaint (“Complaint”) against Defendants Mr. Cooper Group, Inc. (“Mr. Cooper Group”) and Nationstar Mortgage, LLC d/b/a Mr. Cooper (“Nationstar”) (collectively “Defendants” or “Mr. Cooper”) on behalf of himself and all others similarly situated. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences and as to all other matters, upon information and belief, including investigation conducted by his attorneys.

**NATURE OF THE ACTION**

1. Mr. Cooper is a Dallas-based mortgage lending and loan servicing company that boasts its status as the third-largest servicer in the United States, with an estimated 4.3 million customers nationwide.<sup>1</sup> The total value of its portfolio of mortgages loans is \$937 billion.

2. Mr. Cooper was known as Nationstar Mortgage until 2017.<sup>2</sup>

3. Mr. Cooper has revealed that its servers were hacked by cybercriminals in October 2023.<sup>3</sup>

4. Mr. Cooper admitted that the breach was extensive, resulting in the theft of “sensitive information belonging to nearly 15 million current and former customers and applicants.” The extent of the breach was detailed in a report to the Attorney General of Maine:

---

<sup>1</sup> *About Us*, MR. COOPER, <https://www.mrcooper.com/about-us/overview> (last visited Feb. 5, 2024).

<sup>2</sup> <https://www.housingwire.com/articles/40016-its-official-nationstar-will-become-mr-cooper-in-august-2017/>

<sup>3</sup> *Mortgage lender Mr. Cooper admits personal data of millions stolen in October cyberattack*, DELAWARE ONLINE, <https://www.delawareonline.com/story/news/crime/2023/12/21/mortgage-company-mr-cooper-hack-class-action-lawsuit/71983257007/> (last visited Feb. 5, 2024.)

1 In a notice to the Maine Attorney General, the company included a  
2 letter addressed to the 14.7 million impacted consumers. In the letter, it  
3 explained that, beyond Mr. Cooper's customers, the personally  
4 identifiable information was stolen from a wide range of consumers,  
5 including:

- 6 • Those who had a mortgage that was acquired or serviced by  
7 Nationstar Mortgage LLC or Centex Home Equity.
- 8 • Those who had a mortgage that is or was serviced by a sister  
9 brand.
- 10 • Those who have a mortgage from a company whose service  
11 partner is or was Mr. Cooper.
- 12 • Those who applied for a home loan.

13 The letter details that along with names, addresses and phone numbers,  
14 stolen personal information included:

- 15 • Social Security numbers.
- 16 • Dates of birth.
- 17 • Bank account numbers.<sup>4</sup>

18 5. Mr. Cooper's investigation revealed that there was "unauthorized  
19 access to certain of [its] systems between October 30, 2023 and November 1, 2023,"  
20 during which time files containing personal information were exfiltrated and  
21 "obtained by an unauthorized party."<sup>5</sup>

22 6. In response to the breach, Mr. Cooper was forced to shut down its  
23 systems, initially stating on October 31 that its systems were offline due to an

---

24 <sup>4</sup> *Id.*; *Data Breach Notifications*, MAINE ATTORNEY GENERAL,  
25 [https://apps.web.maine.gov/online/aeviewer/ME/40/176a338a-f640-43d5-b975-  
5996823e7ce4.shtml](https://apps.web.maine.gov/online/aeviewer/ME/40/176a338a-f640-43d5-b975-5996823e7ce4.shtml) (last visited Feb. 5, 2024).

26 <sup>5</sup> *Mortgage giant Mr. Cooper hit with cyberattack possibly affecting more than 14 million*  
27 *customers*, ABC NEWS, [https://abcnews.go.com/Politics/mortgage-giant-mr-cooper-hit-  
cyberattack-possibly-affecting/story?id=105745061](https://abcnews.go.com/Politics/mortgage-giant-mr-cooper-hit-cyberattack-possibly-affecting/story?id=105745061) (last visited Feb. 5, 2024).

1 outage. Accordingly, customers were unable to access their accounts or make  
2 mortgage payments.<sup>6</sup>

3 7. On approximately December 15, 2023, Mr. Cooper began notifying  
4 customers that their information had been accessed and exfiltrated by hackers.<sup>7</sup> (See  
5 Plaintiff's Notice of Data Breach, attached hereto as Exhibit A.)

6 8. Though Mr. Cooper has not publicly provided details on the type of  
7 cyberattack that occurred, taking systems offline as Mr. Cooper did on  
8 approximately October 31, 2023 and November 1, 2023 "is the typical response to a  
9 ransomware attack."<sup>8</sup>

10 9. The cyberattack that occurred between October 30, 2023 and November  
11 1, 2023 exfiltrated consumers' sensitive personal data from Mr. Cooper's  
12 network(s), and that data is now in the hands of the perpetrators.

13 10. On information and belief, the information stolen from Mr. Cooper's  
14 network(s) included nonencrypted and nonredacted personal information, as defined  
15 in Cal. Civ. Code § 1798.81.5(A)(1)(d), for Plaintiff Randles and the members of the  
16 alleged Class, including social security numbers and bank account numbers.

17 11. As a result of this data breach, Plaintiff Randles and the members of the  
18 alleged Class face a lifetime risk of identity theft.

19 12. The data breach occurred due to Mr. Cooper's negligent and careless  
20 acts and omissions and the failure to protect consumers' data. Mr. Cooper is  
21 responsible for allowing the data breach to occur because it failed to implement  
22

---

23  
24 <sup>6</sup> Mr. Cooper hackers stole personal data on 14 million customers, TECHCRUNCH,  
25 [https://techcrunch.com/2023/12/18/mr-cooper-hackers-stole-personal-data-on-14-million-](https://techcrunch.com/2023/12/18/mr-cooper-hackers-stole-personal-data-on-14-million-customers/?guccounter=1)  
customers/?guccounter=1 (last visited Feb. 5, 2024).

26 <sup>7</sup> Mr. Cooper Data Breach Impacts 14.7 Million Individuals, SECURITYWEEK,  
27 <https://www.securityweek.com/mr-cooper-data-breach-impacts-14-7-million-individuals/> (last  
visited Feb. 5, 2024).

28 <sup>8</sup> Id.

1 reasonable security procedures and practices and failed to comply with industry-  
2 standard data security practices.

3 13. Mr. Cooper has failed to satisfy its duty under the California Consumer  
4 Privacy Act, Cal. Civ. Code § 1798.100, *et seq.* (“CCPA”) to implement reasonable  
5 security procedures and practices appropriate to the nature of the personal  
6 information in its possession.

7 14. If Mr. Cooper had reasonable security procedures and practices in  
8 place, this incident would not have occurred. Likewise, reasonable security  
9 procedures and monitoring during the breach itself would have mitigated the scope  
10 and impact of the data breach. Mr. Cooper has failed to satisfy its duty under  
11 California law and has violated the CCPA in the process.

12 15. On behalf of himself and all others similarly situated, Plaintiff brings  
13 this case as a class action asserting claims against Mr. Cooper under the CCPA.

14 16. Plaintiff is informed and believes, and upon such information and belief  
15 avers, that this action is based upon a common nucleus of operative fact. This action  
16 is based on the same legal theory, namely liability under the CCPA. This action  
17 seeks relief expressly authorized by the CCPA: (i) injunctive relief enjoining  
18 Defendants from continuing to violate the CCPA; (ii) an award of statutory damages  
19 in an amount not less than one hundred dollars (\$100) and not greater than seven  
20 hundred and fifty (\$750) per Class member for each violation of the CCPA; and any  
21 other relief the Court deems proper as a result of Defendants’ CCPA violations.

## 22 **PARTIES**

23 17. Plaintiff Adrian Scott Randles is a natural person and citizen of the state  
24 of California. He resides in Los Banos, Merced County, California.

1           18. Defendant Nationstar Mortgage, LLC d/b/a Mr. Cooper is a Delaware  
2 limited liability company with its principal place of business located at 8950 Cypress  
3 Waters Blvd, Coppell, TX 75019.

4           19. Defendant Mr. Cooper Group, Inc. is a Delaware corporation with its  
5 principal place of business located at 8950 Cypress Waters Blvd, Coppell, TX  
6 75019. Mr. Cooper Group is the operating parent of its subsidiary, Nationstar.

7                                   **JURISDICTION AND VENUE**

8           20. The Court has subject matter jurisdiction over this action pursuant to  
9 the Class Action Fairness Act, 28 U.S.C. § 1332(d) (“CAFA”). The alleged Class  
10 consists of over 100 persons, there is minimal diversity, and the claims of the class  
11 members when aggregated together exceed \$5 million. Further, none of the  
12 exceptions to CAFA applies.

13           21. This Court has personal jurisdiction over Defendants because  
14 Defendants conduct a significant amount of business in this District and purposely  
15 avail themselves of the privileges of conducting business in this District, service  
16 loans for and collect personal information from customers located in this District,  
17 and because Plaintiff’s claim arises from wrongful conduct that occurred in, was  
18 directed to, and/or emanated from this District, namely the collection of and failure  
19 to protect the sensitive personal information of its customers in California and in this  
20 district.

21           22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1),  
22 (b)(2), and (c)(2) because the Court has personal jurisdiction over Defendants’  
23 actions as stated above, such that it may be deemed to reside in this District, and  
24 because Defendant conducts a significant amount of business within this District and  
25 the wrongful conduct giving rise to this case occurred in, was directed to, and/or  
26 emanated from this District.

**FACTS RELATING TO PLAINTIFF RANGLES**

23. Randles is, and was at all times relevant to this Complaint, a resident of Los Banos, California.

24. Plaintiff Randles has a mortgage loan that, at some time prior to the data breach, was transferred to and serviced by Mr. Cooper.

25. During the course of servicing Plaintiff's loan, Mr. Cooper collected sensitive personal information from Randles, including his name, address, bank account information, and Social Security number.

26. On or around December 16, 2023, Randles received a letter from Mr. Cooper notifying him that his personal information was affected by a "data security incident" at Mr. Cooper. (*See* Randles Notice Letter, attached hereto as Exhibit B, at 2.)

27. The letter informed Mr. Randles that his "name, address, phone number, [and] Social Security number" were included in the files impacted by the breach. (*Id.*)

28. As a result of Mr. Cooper's failure to implement reasonable security procedures, Plaintiff's personal information is forever in the possession of criminal actors who could use the information for any number of improper purposes and scams, including making the information available for sale on the dark web.

**FACTS RELATING TO ALL COUNTS**

29. As stated above, Mr. Cooper's network(s) were infiltrated by hackers between October 30, 2023 and November 1, 2023, which resulted in the exfiltration of nonredacted and nonencrypted personal information of consumers, including Plaintiff.

30. Under the CCPA:

1 Any consumer whose nonencrypted and nonredacted personal  
2 information as defined in subparagraph (A) of paragraph (1) of  
3 subdivision (d) of Section 1798.81.5, or whose email address in  
4 combination with a password or security question and answer that  
5 would permit access to the account, is subject to an unauthorized access  
6 and exfiltration, theft, or disclosure as a result of a business's violation  
7 of the duty to implement and maintain reasonable security procedures  
8 and practices appropriate to the nature of the information to protect the  
9 personal information may institute a civil action for any of the  
10 following:

8 (A) To recover damages in an amount not less than one hundred dollars  
9 (\$100) and not greater than seven hundred and fifty (\$750) per  
10 consumer per incident or actual damages, whichever is greater.

11 (B) Injunctive or declaratory relief.

12 (C) Any other relief the court deems proper.

13 CAL. CIV. CODE § 1798.150.

14 31. The statute defines a “business” as a for-profit corporation or other  
15 legal entity that “collects consumers’ personal information . . . and that alone, or  
16 jointly with others, determines the purposes and means of the processing of  
17 consumers’ personal information” and does business in California. *Id.* §  
18 1798.140(d)(1). The statute further requires that the business meet one of three  
19 threshold requirements: (1) annual gross revenues of more than \$25,000,000 in the  
20 previous calendar year; (2) annual aggregate purchase, sale, or sharing of personal  
21 information of 100,000 or more consumers or households; (3) 50 percent or more of  
22 annual revenues derived from selling consumers’ personal information. *Id.* §  
23 1798.140(d)(1)(A)–(C). The definition further includes any entity that controls or is  
24 controlled by a so-defined business, shares common branding therewith, and  
25 receives shared personal information from the business. (*Id.* § 1798.140(d)(2).  
26  
27  
28



32. The CCPA further defines “processing” as “any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.” *Id.* § 1798.140(q).

33. Defendants are for-profit corporations that do business in California. They collect personal information directly from their customers during the course of their business, including for the purposes of loan servicing and administration, and Defendants themselves determine the purposes and means of processing the data they collect.

34. Defendants also easily exceed the first threshold requirement identified in the CCPA—Mr. Cooper reported annual revenue of \$2.72 billion in 2022 and \$2.15 billion in 2023.<sup>9</sup> Indeed, Mr. Cooper boasted earnings of \$275 million in the third quarter of 2023 alone.<sup>10</sup>

35. Because they meet each element of the statutory definition, Defendants are “businesses” subject to the requirements of the CCPA.

36. In turn, the type of information contained in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 (and thus the subject of this law), includes:

(A) An individual’s first name or first initial and the individual’s last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver’s license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

<sup>9</sup> See <https://companiesmarketcap.com/mr-cooper/revenue/> (last visited Feb. 6, 2024).

<sup>10</sup> *Mr. Cooper Group Reports Third Quarter 2023 Results*, Mr. Cooper Group (Oct. 25, 2023), <https://www.mrcoopergroup.com/press-releases/mr-cooper-group-reports-third-quarter-2023-results/>.

1 (iii) Account number or credit or debit card number, in combination with  
2 any required security code, access code, or password that would permit  
access to an individual's financial account.

3 (iv) Medical information.

4 (v) Health insurance information.

5 (vi) Unique biometric data generated from measurements or technical  
analysis of human body characteristics, such as a fingerprint, retina, or  
6 iris image, used to authenticate a specific individual. Unique biometric  
data does not include a physical or digital photograph, unless used or  
7 stored for facial recognition purposes.

8 (vii) Genetic data.

9 37. On information and belief, and in accordance with the letter received  
10 from Mr. Cooper, Plaintiff Randles's nonencrypted and nonredacted social security  
11 number was exfiltrated from Mr. Cooper's network at the time of the breach at issue.  
His account number and security access code were likely exfiltrated as well.

12 38. On information and belief, Randles's social security number was  
13 subject to an unauthorized access and exfiltration, theft, or disclosure as a result of  
14 Mr. Cooper's violation of its duty to implement and maintain reasonable security  
15 procedures and practices.

16 39. Given the substantial increase in cyberattacks in recent years, and in  
17 light of Mr. Cooper's possession of sensitive personal information pertaining to  
18 millions of consumers across the country, Mr. Cooper's duty to implement  
19 reasonable security procedures and practices is especially important.

20 40. Nevertheless, Mr. Cooper failed to institute reasonable security  
21 procedures and likewise failed to protect consumer data from unauthorized access  
22 and exfiltration.

23 41. As a baseline, the FTC has issued a publication titled "Protecting  
24 Personal Information: A Guide for Business, which establishes fundamental  
25  
26  
27  
28

1 guidelines for businesses to implement data security procedures and practices.<sup>11</sup>

2 Among other practices, the guide suggests that businesses should encrypt sensitive  
3 information stored on their networks, dispose of sensitive information that may no  
4 longer be needed, assess security vulnerabilities in their systems, and limit physical,  
5 internet, and/or network access to servers containing sensitive information,

6 42. On information and belief, Mr. Cooper did not utilize reasonable  
7 security procedures or practices for protecting and monitoring sensitive information,  
8 including but not limited to encrypting sensitive information, limiting access to  
9 servers containing customer personal information, maintaining a secure firewall,  
10 monitoring for suspicious, irregular, or unknown traffic, users, or activity within its  
11 servers, and assessing vulnerabilities in its system.

12 43. As noted above, the breach occurred or began on approximately  
13 October 30, 2023, but it was not discovered until October 31, 2023 and reportedly  
14 continued until November 1, 2023. On information and belief, the implementation  
15 and maintenance of reasonable security practices and procedures would have  
16 prevented and/or mitigated the scope and extent of the breach.

17 44. As a result of Mr. Cooper's failure to implement reasonable security  
18 practices and procedures, Plaintiff and the Class's personal identifying information  
19 is now in the hands of hackers, who could use or sell their data in any number of  
20 ways that could cause substantial damage to a person's identity or credit history.

21 45. Plaintiff and the class members have experienced injury, including a  
22 substantial increase in the likelihood of identity theft; the compromise, publication,  
23 and theft of their personal information; the continued risk to their personal  
24 information; future costs in terms of time, effort, and money that will be required to  
25

---

26 <sup>11</sup> *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016),  
27 [https://www.ftc.gov/business-](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business)  
28 [guidance/resources/protecting-personal-information-guide-business](https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business) (last visited Feb. 6, 2024)

1 prevent, detect, and repair the impact of the personal information compromised as a  
2 result of the data breach; and loss of value to their personal information.

### 3 **CLASS ALLEGATIONS**

4 46. **Class Definitions:** Plaintiff brings this class action on behalf of himself  
5 and a Class of similarly situated individuals, defined as follows:

6 All persons residing in California whose nonredacted and nonencrypted  
7 personal information was compromised in the data breach(es) affecting  
8 Mr. Cooper's network(s) in 2023.

9 Excluded from the Class are (1) Defendants, Defendants' agents, subsidiaries,  
10 parents, successors, predecessors, and any entity in which Defendants or their parent  
11 have a controlling interest, and those entities' current and former employees,  
12 officers, and directors, (2) the Judge or Magistrate Judge to whom this case is  
13 assigned and the Judge's or Magistrate Judge's immediate family, (3) persons who  
14 execute and file a timely request for exclusion, (4) persons who have had their  
15 claims in this matter finally adjudicated and/or otherwise released, and (5) the legal  
16 representatives, successors, and assigns of any such excluded person.

17 45. **Numerosity:** The exact number of Class members is unknown to  
18 Plaintiff at this time, but it is clear that joinder of each individual member is  
19 impracticable. Defendants have indicated that the breach may have impacted more  
20 than fourteen million customers across the country.

21 46. **Commonality:** Common questions of law and fact exist as to all  
22 members of the Class for which this proceeding will provide common answers in a  
23 single stroke, including:

24 a. Whether Mr. Cooper implemented and maintained reasonable  
25 security procedures and practices appropriate to the nature of storing Plaintiff's and  
26 the Class members' personal information;

1           b.     Whether Mr. Cooper knew or should have known that it had  
2 failed to implement and maintain reasonable security procedures and practices to  
3 keep Plaintiff's and Class members' personal information secure and prevent loss,  
4 exfiltration, or misuse of that information;

5           c.     Whether Mr. Cooper adequately addressed and fixed the  
6 vulnerabilities which permitted the data breach(es) to occur;

7           d.     Whether Mr. Cooper has cured the alleged violation; and

8           e.     Whether Plaintiff and the Class members are entitled to relief and  
9 the nature of such relief.

10         35.    **Typicality:** As a result of Defendants' uniform conduct, acts, and  
11 omissions with respect to the consumer information it possessed, Plaintiff and the  
12 Class members suffered the same injury and similar damages. Thus, Plaintiff's  
13 claims are typical of the claims of the other Class members.

14         36.    **Adequate Representation:** Plaintiff is a member of the Class and both  
15 he and his counsel will fairly and adequately represent and protect the interests of  
16 the Class, as neither has interests adverse to those of the Class members and  
17 Defendants have no defenses unique to Plaintiff. In addition, Plaintiff has retained  
18 counsel competent and experienced in complex litigation and class actions,  
19 including class actions focused on privacy laws. They have the ability to prosecute  
20 the case and the financial resources to do so.

21         37.    **Injunctive and Declaratory Relief:** In using uniform (inadequate)  
22 security procedures, Mr. Cooper has acted or refused to act on grounds generally  
23 applicable to the Class a whole so as to render injunctive and declaratory relief  
24 appropriate. Stated differently, Defendants' uniform conduct requires the Court's  
25 imposition of uniform relief to ensure compatible standards of conduct toward the  
26 Class members, thus making final injunctive and/or declaratory relief appropriate  
27  
28

with respect to the Class as a whole. Further, because Defendants’ uniform practices result in similar, if not identical, injuries for all Class members, Plaintiff’s challenge of those practices hinges on Defendants’ conduct with respect to the Class, not on facts or law applicable only to Plaintiff.

38. **Predominance:** The common questions of law and fact set forth above go to the very heart of the controversy and predominate over any supposed individualized questions. Irrespective of any given Class member’s situation, the answer to whether Defendants’ security procedures, if any, constituted “reasonable” procedures and practices in accordance with its duty under the CCPA is the same for each class member and will be proven using common evidence.

39. **Superiority and Manageability:** A class action is superior to all other methods of adjudicating the controversy. Joinder of all claims is impractical, and the damages suffered by/available to the individual Class members will likely be small relative to the cost associated with prosecuting an action. Thus, the expense of litigating an individual action will likely prohibit the Class members from obtaining effective relief for Defendants’ misconduct. In addition, there are numerous common factual and legal questions that could result in inconsistent verdicts should there be several successive and differing trials. In contrast, a class action will present far fewer management difficulties, as it will increase efficiency and decrease expense. Further, class-wide adjudication will also ensure a uniform decision for the Class members.

40. Plaintiff reserves the right to revise the definition of the Class as necessary based upon information learned in discovery.

### **FIRST CAUSE OF ACTION**

#### **Violations of the California Consumer Privacy Act Cal. Civ. Code § 1798.100, et seq. (On behalf of Plaintiff and the Class)**

1           41. Plaintiff incorporates by reference the foregoing allegations as if fully  
2 set forth herein.

3           42. The CCPA went into effect on January 1, 2020. This privacy law was  
4 enacted to protect consumers' personal information.

5           43. Defendants are "businesses" as that term is defined in the CCPA, and  
6 they are therefore subject to liability under the statute.

7           44. Mr. Cooper violated CCPA Section 1798.150(a) by violating its duty to  
8 implement and maintain reasonable security procedures and practices appropriate to  
9 the nature of the personal information in its possession for both Plaintiff and Class  
10 members.

11           45. As a result of Defendants' violation of its duty, Plaintiff's and Class  
12 members' nonencrypted and nonredacted personal information was exfiltrated and  
13 subject to unauthorized disclosure.

14           46. In accordance with Civil Code Section 1798.150(b), Plaintiff sent to  
15 Defendants, via email and overnight United Parcel Service, notice of these CCPA  
16 violations and a demand for relief, more than thirty days prior to the filing of this  
17 Complaint.

18           47. On behalf of Class members, Plaintiff seeks injunctive relief in the form  
19 of an order enjoining Defendants from continuing to fail to implement reasonable  
20 procedures to protect Plaintiff's and the Class's personal information.

21           48. Plaintiff also seeks statutory damages in an amount not less than one  
22 hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per  
23 consumer per incident, attorneys' fees and costs, and any other relief the Court  
24 deems proper.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff Randles, on behalf of himself and the Class, respectfully requests that this Court issue an order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff as class representative and appointing his counsel as class counsel;

B. Declaring that Defendants' actions, as set out above, constitute violations of California law;

C. Awarding damages, including punitive damages where applicable, to Plaintiff and the Class in amounts to be determined at trial, to be paid into a common fund for the benefit of the Class;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, *inter alia*, an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

E. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable;

G. Providing such other injunctive and/or declaratory relief as is necessary to protect the interests of Plaintiff and the Class; and

H. Awarding such other and further relief as equity and justice may require.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury for all claims so triable.

Respectfully submitted,



1 Dated: February 6, 2024

**ADRIAN SCOTT RANGLES**, individually  
and on behalf of all others similarly situated,

2  
3 By: /s/ Rebecca Davis

4 One of Plaintiff's Attorneys

5  
6 Rebecca Davis (SBN 271662)

7 rebecca@lozeaudrury.com

**LOZEAU DRURY LLP**

8 1939 Harrison Street, Suite 150

9 Oakland, California 94612

10 Telephone: (510) 836-4200

11 Facsimile: (510) 836-4205

**WOODROW & PELUSO, LLC**

12 Patrick H. Peluso\*

13 ppeluso@woodrowpeluso.com

14 3900 East Mexico Avenue, Suite 300

15 Denver, Colorado 80210

16 Telephone: (720) 213-0675

17 Facsimile: (303) 927-0809

18 Attorneys for Plaintiff and the Class

19  
20 \* *Pro Hac Vice admission to be sought*